Legal Implications of the General European Data Protection Regulation

Michael Hopp

PLESNER

Agenda

Brief introduction to the New Regulation

1. Extract of the GDPR compared to the current directive
2. Accountability
3. Privacy by design // Privacy by default
4. Data Breach notification
5. What to do before the new regulation enters into force

Extract of the GDPR compared to the current directive

- Changes to the rules regarding processing
- Increased number of derogations
- Strengthening data subjects' rights
- Meta-rules
- Burdensome obligations on data processors
- Closer co-operation between DPAs
- Significant fines

Accountability – article 22

(Council)

"Taking into account the nature, scope, context and purpose of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall implement appropriate measures and be able to demonstrate that the processing of personal data is preformed in compliance with this regulation".

- Risk based approach
  - "Taking into account …"
  - the circumstances of the processing, and the likelihood and severity of risk for the data subject
- Obligations
  - "implement appropriate measures"
  - "be able to demonstrate … compliance with this regulation"
- Applies to all requirements under the GDPR
  - Ordinary requirements and security requirements
- Does NOT introduce risk-based compliance with the ordinary requirements. Only risk-based accountability.
- Violation subject to fines (3rd bracket)

Data protection impact assessment - article 33

(Council) 1. Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

- Risk-based approach
- Up-front compliance analysis
  - Ordinary requirements and security requirements
- Closely related to accountability and security
  - The mitigating actions identified in the PIA will also be triggered under article 22 or article 30
- Violation subject to fines (3rd bracket)

Privacy by design // Privacy by default

Article 23 - Data protection by design and by default (Council)

1. Having regard to available technology and the cost of implementation and taking account of *the nature, scope, context and purposes of the processing* as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation, in such a way that the processing will meet the requirements of this Regulation and protect the rights of data subjects.

- Risk-based approach
- "… measures appropriate"
- A sub-set of accountability

2. The controller shall implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

- NOT risk-based – "ensuring that"
- But still "appropriate measures"
- A sub-set of accountability

Security (is not a meta-rule) – article 30

(Council:)

1. Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures, such as pseudonymisation of personal data to ensure a level of security appropriate to the risk.

1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

- Risk based approach
  - "Having regard" and "taking into account …"
  - the circumstances of the processing, and the likelihood and severity of risk for the data subject
- Security obligations are inherently risk-based – as opposed to the material obligations
- Obligations
  - "implement appropriate technical and organisational measures"
  - "to ensure a level of security appropriate to the risk"
- Applies to controllers and processors

PLESNER

Data Breach Notification – article 31-32

- Notification of data breaches to the DPA and to the data subjects
  - Council: "[if] a personal data breach which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage [occurs, then obligation to notify]"
- Risk-based approach – main focus on consequences of data breach
- Deadline: "Without undue delay" (normally within 72 hours)
- Exception - article 32(3):
  - Anonymous data
  - Subsequent compensational steps
  - Disproportionate effort
  - Public interests
- Violation subject to fines (3rd bracket)

What to do before the GDPR enters into force

- Understand the distinction between the general requirements and the meta-rules
- Establish a task force that can prepare the implementation of the GDPR. Members: Legal, IT, InfoSec, HR and Marketing
- Establish an overview of the categories of personal data and the purposes that the data is being used for
- Identify all policies currently in force
- Are the consent wordings valid? Now and in the future…
- Map your data processing agreement
- Collect information about your vendor management of data processors
- Get an overview of ongoing or near-future IT projects
- Prepare a data breach handling procedure
- Keep the difference between compliance and security in mind


Questions
PLESNER

Our team

Michael Hopp
Attorney-at-Law, Partner

Data Protection Law
Technology, Media and Telecoms (TMT)
E-commerce

T: +45 36 94 13 06
M: +45 29 99 30 14
E: mho@plesner.com

Christian Wiese Svanberg
Attorney-at-Law

Data Protection Law
Technology, Media and Telecoms (TMT)
E-commerce

T: +45 36 94 11 96
M: +45 30 93 71 10
E: cws@plesner.com

Martin Hjørlund Nielsen
Assistant Attorney

Data Protection Law
Technology, Media and Telecoms (TMT)
E-commerce

T: +45 36 94 11 89
M: +45 30 93 71 85
E: mhd@plesner.com

Ulrik Birk Gotfredsen
Assistant Attorney

Data Protection Law
Technology, Media and Telecoms (TMT)
E-commerce

T: +45 36 94 14 25
M: +45 30 93 72 08
E: ubg@plesner.com

Martin Nybye-Petersen
Assistant Attorney

Data Protection Law
Technology, Media and Telecoms (TMT)
E-commerce

T: +45 36 94 15 21
M: +45 29 99 30 89
E: mny@plesner.com

Mads Toftgaard Nielsen
Assistant Attorney

Data Protection Law
Technology, Media and Telecoms (TMT)
E-commerce

T: +45 36 94 15 19
M: +45 31 20 92 40
E: mtn@plesner.com